International Journal of Engineering Research (ISSN : 2319-6890)
Volume No.2, Issue No.3, pp : 194-200 01 July 2013

A Review of Different Techniques on Digital Image Watermarking Scheme

Y. Shantikumar Singh[1], B. Pushpa Devi[2], and Kh. Manglem Singh[3]

[1] Department of ECE, [3]Department of CSE, [1, 3] NIT, Manipur, India
[2] Department of ECE, [2] NIT, Meghalaya, India
[1]yshantikumar99@gmail.com, [3]manglem@gmail.com, [2]pushpabmw@gmail.com,

Abstract – In this paper we aim to present a survey of different techniques on digital image watermarking. Digital watermarking technique is becoming more important in this developing society of internet. Digital watermarking is used as a key solution to make the data transferring secure from illegal interferences. Digital watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. In this paper we mainly discussed about two methods via spatial domain and frequency domain. In spatial (pixel) domain, watermark is inserted directly by modifying the pixel values of host image. Such algorithms are very easy at the time of implementation. However they have some problems like Low hiding capacity of watermark information, less PSNR, less correlation between original and extracted watermark and less security, so anyone can detect such algorithms. In frequency domain such as DCT, DFT, DWT, SVD etc, the watermark is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against watermarking attacks because information can be spread out to entire image.

Keywords - Digital Image Watermarking, DCT, DWT, SVD and Algorithm.

I. INTRODUCTION

Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [1]. Various digital watermarking techniques are purposed for copyright protection of multimedia data from being misused [2, 3]. According to the embedding domain of the host image, digital image watermarking techniques can be categorized into one of the two domains via spatial and transform. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [4]. In capacity of data hiding is high in these methods but hardly robust. Watermarking in transform domain is more secure and robust to various attacks. The popular transform domains are frequency domain via Discrete Fourier Transform (DFT) [5], and Singular Value Decomposition (SVD) [10, 11, 12, 13] etc. Normally all popular methods use any of them or their popular variants for providing robust watermarks along with other methods like neural network, vector quantization and many more different distribution functions. Watermarking using DWT and SVD methods are known to have gained much more popularity than any other methods.

A well known matrix decomposition method as Singular Value Decomposition (SVD) is widely used in watermarking techniques. In this technique the watermark is embedded did to the SV (s) of the whole image or a part of it. In this technique a single watermark is used which may be lost due to attacks [11]. To improve this work [15] on DWT-based multiple watermarking argues that inserting a visual watermark in both low and high valued coefficients results in a robust technique for a wide range of attacks. The robustness is increased by inserting in low valued coefficients with respect to attacks that have low pass characteristics such as filtering, lossy compression.

Digital watermark is a technique that is embedded inside an image. It is very similar to steganography in a number of respects. The main aim of digital image watermarking is to embed information imperceptibly and robustly in the cover data.

This survey paper is discussed in the following sections. In section 2 we discuss the different techniques of digital image watermarking. In section 3 we discuss the applications of Digital Image Watermarking. In section 4 we discuss the attacks on digital image watermarking. We conclude this survey in section 5.

II. DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

Watermarking is not a new phenomenon. In the modern era, providing authenticity is becoming increasingly important as most of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer [31]. Watermarking algorithms are divided into two categories. Spatial-domain techniques work with the pixel values directly. Frequency-domain techniques employ various transforms, either local or global. Several widely recognized techniques are described subsequently [32].

A. Spatial Domain Techniques

In this technique, the watermark is inserted in the cover image changing pixels or image characteristics [33]. The algorithm should carefully weight the number of changed bits in the pixels against the possibility of the watermark becoming visible [34]. Mahfuzur Rahman and Koichi Harada proposed a

International Journal of Engineering Research (ISSN : 2319-6890)
Volume No.2, Issue No.3, pp : 194-200 01 July 2013

method to insert information in objects with layered 3D triangular meshes such as those reconstructed from CT or MI data, a parity enhanced topology based spot area watermarking method [31]. The robustness against unauthorized alteration of a single bit in every consecutive 8-bits of length is enhanced by the incorporation of parity checking. Watermark message is cut into numerous pieces and each piece of message is inserted at different spots, hence, if a piece of message is lost in one spot, the error correct decoding can be employed to possibly retrieve the same information from other spots. Their method acted against unintentional attacks translation, rotation, arbitrary re-sectioning, scaling etc, and left artifact after intentional attacks of local and global number re-arrangement in a robust manner. This method has the ability to check the alteration of a single bit in every consecutive 8-bits length as it is parity enhanced.

Xiangui Kang et al. [35] proposed the data extraction process as one associated with a generalized channel of additive noise with a generally non-zero mean and fading by adaptively estimating the decision zone exploiting a training sequence and estimating the quantization step size using the Fourier analysis method. Their approach functions against common signal processing including Gaussian filtering, mean filtering, median filtering, sharpening, and jpeg compression with a quality factor of as low as 10, robustly. The main progress is the enhanced robustness against median filtering, intensity DC change, intensity linear scaling, colour reduction, histogram equalization and intensity non-linear scaling, etc. in comparison with the watermarking scheme described in [36] which does not employ adaptation. The proposed scheme has more superior robustness to additive noise corruption, jpeg compression, median filtering, and accomplishes much enhanced watermark invisibility simultaneously in comparison to the scheme proposed in [37].

C. Lu, H.Yuan and M. Liao [38] presented a multipurpose watermarking scheme which can be applied to attain both authentication and protection of multimedia data. The hiding process inserts the watermark once which can be extracted for diverse applications in the direction process, invisibly. Their proposed includes the following three special features a) The approximation information of a host image kept in the hiding process by utilizing masking thresholds defined based on the human visual system, b) oblivious and robust watermarking accomplished, c) a asymmetric robust range adopted for fragile watermarking to achieve malicious tampering detection and non-malicious tampering tolerance.

Ruizhen Liu and Tieniu Tain presented a new watermarking method for digital images [39]. The SVD domain of the original image is added with the watermark. The mathematical background of their method is very apparent and the estimation of the error between the original image and the watermarked image is performed. The performance of this novel algorithm is good in terms of both security and robustness owing to these properties. Moreover, their algorithm can resolve rightful ownership devoid of encryption and if combined with encryption, they can provide more powerful security for rightful ownership. They performed extensive experiments and employed Cox method [1] for comparison. The robust nature of the novel method against image distortion and its significant superiority over Cox method is illustrated by the results.

Wei Lu and Hongtao Lu [40] provided a novel robust digital image watermarking scheme with the aid of sub-sampling and nonnegative matrix factorization. Originally, sub-sampling is employed to create a sub-image sequence. Later, the nonnegative matrix factorization is applied to decompose the sequence on basis of the column similarity of the sub-image sequence. A Gaussian pseudo-random watermark sequence is embedded in the factorized decomposition coefficients. Owing to the high resemblance of sub-images and meaningful factorization for NMF, the purposed scheme is capable of achieving superior robustness, particularly towards common permutation attacks.

Lin et al [41] proposed a method to solve the problems of rotation, scale, and translation. Their solution and the prior proposals in the pattern recognition literature regarding invariants of the Fourier-Mellin transform are associated. They observed that the random transform can be employed for alternative implementation [42]. Their technique is resilient against mild jpeg compression as well. In addition, the efficiency of their method against cropping, an attack against which no steps are taken in the design and illustrated through the results.

1) Least Significant Bits (LSB): This is the simplest approach, because the least significant bit carries less relevant information and their modification does not cause perceptible changes. Among these approaches there are types using only the salient points [43] or types, which use some kind of cryptography on the watermark message before the embedding, process [44].

2) SSM Modulation Based Techniques: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for different reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

B. Frequency Domain Techniques

Compared to spatial domain techniques, frequency domain techniques are more applied. The target of this technique is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The discrete wavelet transforms (DWT) and the discrete cosine transforms (DCT) are implemented very effectively in numerous digital images watermarking scheme. In this new era Singular Value Decomposition (SVD) is also implementing very effectively in the digital image watermarking scheme. Al-Haj [45] presented a combined DWT-DCT digital image watermarking algorithm. Watermarking is carried out through the embedding of the watermark in the first and second level DWT sub-bands of the host image sub-sequenced by the application of DCT on the

selected DWT sub-bands. The most commonly used transforms are given below:

1. Discrete Cosine Transform (DCT)

Discrete Cosine Transform is like as Discrete Fourier Transform. It is a technique for converting a signal into elementary frequency components [16]. The 2-dimentional DCT of given matrix gives the frequency coefficients in the form of another matrix. The left topmost corner of the matrix represents the lowest frequency coefficients while the right bottom most corner represents the highest frequency coefficients. Watermarking with DCT techniques are robust as compared to spatial domain techniques. Such algorithms are robust on image processing operation like low pass filtering, brightness and contrast adjustment, blurring etc. However they are weak against geometric attacks like rotation, scaling, cropping etc. Watermarking with DCT can be divided into Global DCT watermarking and Block based DCT watermarking. For Global DCT watermarking, the transform is applied to all part of the image, separating the spectral regions according to their energy.

We list the algorithm steps purpose by V.M. Potdar, S.Han and E. Chang [17]:

- Segment the image into non-overlapping blocks of 8 x 8.
- Apply forward DCT to each of these blocks.
- Apply some block selection criteria.
- Apply coefficient selection criteria.
- Embed watermark by modifying the selected coefficients.

Apply inverse DCT transform on each block. The technique proposed by R. Mehul and R. Priti [15] provide the watermark is inserted in four different frequency ranges by selecting coefficients in zigzag order. This technique produced good results when attacks are applied but failed to achieve robustness to both compression and image processing tasks simultaneously when only one copy of watermark is inserted.

The technique proposed by J.R Hernandez, M. Amado and F.Perez Gonzalez [18] presents that if the watermark is inserted in perceptually most significant components, i.e., low frequencies; the technique tends to be robust to attack but it is difficult to hide the watermark. On the other hand, if the watermark is inserted in perceptually insignificant components, i.e., high frequencies; it is easier to hide the watermark but the technique is then less resistant to attacks.

The technique proposed by Y. Yang, X. Sun, H. Yang, and C.T. Li [19] present a DCT domain based removable visible watermarking algorithm that moderately succeeds in defeating illegal removal and resisting compression. They intended to protect the multimedia content and to ensure that the reconstructed images are high quality for authorized user, or else, of low-quality for unauthorized users by embedding the visible watermark. Their technique enabled preventing the embedded visible watermark from being illegally removed by unauthorized users without correct user keys as their proposed scheme. In conclusion, the watermarked image is generated by adaptive addition of the significant DCT coefficients of the pre-processed watermark and the corresponding host image. The watermarking system is somewhat robust against compression. They show the performance of their proposed technique the success of the introduced scheme in preventing the inserted watermark from illegal removal is illustrated through the results.

The idea proposed by I.J.Cox, J.Kilian, F.T.Leighton and T.Shamoon [20] present the host image and the watermark communication channel and a signal to be transmitted, respectively. The perceptually important part of signal spectrum is spectrum with the watermark message. Gaussian noise like watermarks is employed to accomplish security. The watermarked image will be damaged if an attempt is made to destroy the watermark.

A method called Optional differential energy watermarking of DCT encoded images and video is proposed by Langelaar and Langendijk [21]. A block which composes of several 8x8 DCT blocks is inserted with a watermark bit by dividing the block into two parts. In order to produce an energy difference in the two parts of the same block, where the energy difference is determined by the watermark bit, the High frequency DCT coefficients in the compressed bit stream are selectively discarded. The number of 8x8 DCT blocks in a block, JPEG quantization, step size, and a minimal cut-off index for watermarking are the three parameters in this technique.

In this [16] techniques, they proposed technique that inserts the watermark into image and extracts the watermark from the watermarked image more efficiently by exploiting the zero-tree in the rearranged DCT coefficients. This technique is reasonable to apply in a real time system as it can directly extract the inserted watermark from the watermarked image devoid of the original image.

A robust digital image watermarking using hybrid DWT-DCT-SVD technique [22] is proposed by S.Murty and P.R.Kumar. They apply DCT to an image results in three frequency sub-bands: low-frequency, mid-frequency and high-frequency sub-bands. They calculated the DCT coefficients for the transformed output image by using Equation 1.

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)cos\left[\frac{(zx+1)u\pi}{2N}\right]cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad [1]$$

$$\text{for } u,v = 0,1,2 \ldots\ldots\ldots\ldots N-1$$

Where

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0 \\ 1, & u = 1,2,\ldots\ldots,N-1 \end{cases}$$

$$\alpha(v) = \begin{cases} \frac{1}{\sqrt{2}}, & v = 0 \\ 1, & v = 1,2,\ldots\ldots,N-1 \end{cases}$$

In the above equation, x is the input image having N x M pixels, $x(m,n)$ is the intensity of the pixel in row m and column n of the image, and $y(u,v)$ is the DCT coefficient in row u and column v of the DCT matrix.

2. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform is a mathematical tool for hierarchically decomposing an image. It is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelet transform provides both frequency and spatial description of an image. The wavelet transform decompose the image in four channels (LL, HL, LH and HH) with the same bandwidth thus creating

a multi-resolution perspective. Due to this advantage the watermark can embed in any of the frequency bands and on inverse transform the watermark will be distributed throughout the low and high frequencies as well as in the spatial domain. DWT is used a lot for watermarking and copyright protection by Shang-Lin Hsieh et al [23] [24] and many other like them [25] [26].

In DWT, the most prominent information in the signal appears in high amplitudes and the less prominent information appears in very low amplitudes. Data compression can be achieved by discarding these low amplitudes. When the DWT is applied to an image, the resolution is reduced by a 2^K, where K is the number of timed the transform is applied.

These algorithms are called the "wavelet based watermarking" [17]. The watermark is inserted by substituting the coefficients of the host image for the watermark data. This method improves mark robustness, but depends on the frequency.

Digital watermarking in wavelet domain presented by Taskovski et al. [27]. They implemented two watermarks using binary marks in LL2 and HH2 respectively, resulting in a mark which is robust against manipulations like compression and weak against cropping and rescaling.

G. Hai-ying et al [28] presented a watermark adapted to JPEG2000 using two algorithms to modify the wavelet coefficients of the LH2 band of the cover image, introducing only minimal differences between the watermarked image and the original.

E.Ganic and A. M. Eskicioglu [30] proposed an algorithm that applies the SVD in all bands of the first level of DWT, making this a watermarking process in all frequencies. They also present the algorithm with greater robustness against cropping, Gaussian noise and compression. Initially, the DWT is applied to HL1or HH1. In selected band, HH2 or HL2 must be selected and divided into 4 x 4 blocks. Finally, SVD is applied to each block, and the watermark is embedded into the S matrix.

3. Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is a numeric analysis of linear algebra which is used in many applications in image processing. It is used to decompose a matrix with a little truncate error according to the equation below:

$$A = USV^T \quad [2]$$

Where A is the original matrix, U and V is orthogonal matrices with dimensions M x M and N x N respectively, S is a diagonal matrix of the Eigen values of A and T indicates matrix transposition. R.Liu and T.Tan [11] did the decomposition of the cover image and added the watermark using a scale coefficient α to get the following equation:

$$S + \alpha W = U_W S_W V_W^T \quad [3]$$

Multiplying matrices U, V^T and S_W result in the marked image A_W:

$$A_W = US_W V^T \quad [4]$$

This is possible due to the high stability of singular value of SVD. In another approach, the cover image is separated in blocks and the SVD applied to each block [46], in this case the dimension of watermark must be equal to the block size and a copy of the watermark is embedded in each block. This technique improves watermark robustness and resistance against many kinds of attacks.

Singular Value Decomposition technique is shown to be powerful methods for robust image watermarking [47], [48]. This can be attributed to the facts that:

- Singular value (SV) of a digital image is stable. The SVs remain intact when disturbances are added to an image.
- SVD preserves both one-way and non-symmetric properties, which are not obtainable using DCT or DFT transformations.
- SVs are able to represent intrinsic algebraic properties of a digital image.
- SVD can be performed on both square and rectangular matrices.

Chandra et al. [14] proposed a method based on the SVD of both the host image and visual watermark. The SVs of the watermark are multiplied by a scaling factor and added to the SVs of the host image. The attacks used are JPEG and low pass filter. However this method is non-blind in nature.

Sun et al. [12] proposed a method based on SVD watermarking scheme, wherein the D component with a diagonal matrix is explored for embedding. The basic mechanism used is the quantization of the largest component with a fixed constant integer, called quantization coefficient. A trade-off can be achieved between transparency and robustness by varying the quantization coefficient. However, this method is failed in extracting the watermark with zero error rates.

Chin-Chen Chang et al. [13] proposed a watermarking scheme based on the SVD domain. U matrix of SVD is used for the watermark embedding. The absolute difference between the two rows of U matrix is used for the watermark embedding. They explored the positive relationships between the rows of U and V matrices that are preserved after JPEG compression also.

Chung et al. [49] proposed two notes on the SVD based watermarking algorithm. From their method, if the watermark is embedded in the columns of U matrix and rows of V^T, the perceptibility of the host image is improved. However, their method is not robust to many attacks since watermark embedding is in U and V^T matrices.

Singular values represent the algebraic properties of an image [50]. Singular values possess the algebraic and geometric invariance to some extent. The properties of the singular values are reviewed as follows.

- Property 1 (SVD): If $A \in R^{mxn}$, then there exist orthogonal matrices $U = [u_1, \dots, u_m] \in R^{mxn}$ and $V = [v_1, \dots, v_n] \in R^{mxn}$ Such that $U^T AV = diag(\sigma_1, \dots, \sigma_p)$. Where, $p = \min(m, n)$, $\sigma_1 \geq \sigma_2 \geq \cdots \sigma_p \geq 0$. $\sigma_i, i = 1,2, \dots p$ are the singular values of A. The singular values are the square roots of the eigen values λ_i of AA^H or $A^H A$, that is $\sigma_i = \sqrt{\lambda_i}$
- Property 2 (The Stability of SV): The stability of singular value indicates that, when there is a little disturbance with A, the variation of its singular value is not greater than 2-norm of disturbance matrix. 2-norm is equal to the largest singular value of the matrix.
- Property 3 (The Scaling Property): If the singular values of A^{mxn} are $\sigma_1, \sigma_2, \dots, \sigma_k$, the singular values of $\alpha * A^{mxn}$ are $\sigma_1^*, \sigma_2^*, \dots \sigma_k^*$, then $|\alpha|(\sigma_1, \sigma_2, \dots \sigma_k) = (\sigma_1^*, \sigma_2^*, \dots \sigma_k^*)$ [5]

- Property 4 (The Rotation invariant Property): If P is a unitary and rotating matrix, the singular values of PA (rotated matrix) are the same as those of A.
- Property 5 (The Translation invariance property): The original image A and its rows or columns interchanged image have the same singular values.
- Property 6 (The Transposition invariance property):If $AA^T u = \lambda^2 u$ then,
  $A^T AV = \lambda^2 v,$ [6]
  so that A and A^T have same singular values.

The above mentioned properties of SVD are very much desirable in image watermarking. When the watermarked image undergoes attacks like rotation, scaling and noise addition, the watermark can be retrieved effectively from the attacked watermarked image due to the above said properties

III. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

In this section we present the review of some common applications before discussing watermarking algorithms.

1) Broadcasting Monitoring: This type of monitoring is used to confirm the content that is supposed to be transmitted [51], [52] and [17]. As an example, commercial advertisements could be monitored through their watermarks to confirm timing and count.

2) Owner Identification: The conventional form of intellectual ownership verification is a visual mark. But, nowadays, this is easily overcome by the use of software that modifies images. An example is images with a copyright registration symbol © which have this mark removed by specialized software. In this case invisible watermarks are used in order to overcome the problem.

3) Fingerprinting: A watermarked object contains information about the owner permissions. Several fingerprints can be hosted in the same image since the object could belong to several users [52], [17].

4) Publication Monitoring and Copy Control: The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software able to update the watermark at every use [52]. It also allows copy tracking of unauthorized distribution since owner data is recorded in the watermark.

5) Image and Content Authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are inserted and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summery of the content. If any part of the content is modified, its summery, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera [53].

6) Temper Detection: Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted [54].

7) Medical Application: Name of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [55].

8) Copyright Protection: Watermarking is essentially applied for copyright protection. The aim is to evade other parties from claiming the copyright by embedding the information that identifies the copyright owner of the digital media. The application must make certain that embedded watermark cannot be eliminated without causing a noteworthy deformation in digital media though maintaining a high level of robustness. It is important to consider further necessities in addition to robustness. For instance, the watermark must ably determine rightful ownership if other parties embed additional watermarks and also explicit by nature. When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

9) Content Description: This watermark can contain some detailed information of the host image such as labeling and captioning. For this kind of application, capacity of watermark should be relatively large and there is no strict requirement of robustness.

10) Convert Communication: The embedded signal is employed in the transmission of secret information from one person (or computer) to another, devoid of anyone along the way becoming aware that this information is being transmitted [59]. It includes exchange of messages secretly inserted within images. In this case, the main requirement is that hidden data should not raise any suspicion that a secret message is being communicated.

11) Signatures: The content owner is recognized by the watermark. It is possible that this might be exploited by a potential user to get hold of legal rights to copy or publish the content from the contact owner.

IV. ATTACKS ON WATERMARKING

The transmission media can cause some loss in the signal implying in a damaged content. These attacks may be intentional or accidental [52]. Intentional attacks use all available resources to destroy or modify the watermark making it impossible to extract it, the methods usually used are: signal processing techniques, cryptanalysis, steganalysis. On the other hand, accidental attacks are inevitable, because every image processing or transmission noise may introduce distortions. Besides these types, there are other types of attacks called estimation based on attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods. Testimation based attacks can be classified as removal, protocol, or desynchronization depending on the way the estimate is used [57].

1) Removal and Interference Attacks: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Moreover,

interference attacks are those which an additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging and noise storm are some examples of this category of attacks. The collusion attack occurs when a number of authorized recipients of the multimedia object come together to generate an un-watermarked object by averaging all the different watermarked objects.

2) Geometric Attacks: Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. This type of attack includes affine transforms such as rotation, translation, and scaling. Warping, line/column removal and cropping are also included in this family of attacks. Another example of geometric attack is the mosaic attack. In this mosaic attack, the watermark image is divided into several parts and rearranged using proper HTML code, constructing watermark image in which the watermark detector will fail to provide desired results. Local pixel jittering is an efficient spatial domain geometric attack.

3) Cryptographic Attacks: The above two types of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security. For example, finding the secrete watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [55]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

4) Protocol Attacks: The protocol attacks exploit the loopholes in the watermarking concept. One example of such attack is the IBM attack [58]. The IBM attack is also known as the deadlock attack, inversion attack, or fake-original attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarking of an already watermarked image is called re-watermarking. In some inversion attacks, a fake original object is created that produces the same results through the detector as that of the real original object.

Hartung et al. [59] also classified these attacks in classes:

5) Simple Attacks: These attacks change the data of the cover image without attempting to target the watermark location. Example: Noise addition, cropping, conversion to analog and wavelet-based compression.

6) Disabling Attacks: The goal of these attacks is to attempt to break the correlation between the watermark and the cover image, making extraction impossible. Example: Geometric distortions, rotation, cropping and insertion of pixels.

7) Ambiguity Attacks: These attacks confuse the receptor by embedding a fake watermark, making it impossible to discover which the original embedded mark in the cover image was.

8) Removal Attacks: In this type of attack a study of the watermark is carried out, estimating the watermark content and attempting to separate it from the host image. Example: Certain non-linear filter operations and attacks tailored to a specific watermark algorithm.

V. CONCLUSION

In this paper, we have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD. These marks are robust against several different attacks. In this paper we also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented.

In future works, the use of coding and cryptography watermarks will be approached. There is a large amount of literature on these topics showing that the robustness increments can be gained through the addition of coding techniques.

ACKNOWLEDGEMENT

The author thanks L. Surajkumar Singh, Assistant Professor of Electronics and Communication Engineering, NIT Manipur for his guidance and active support during the progress of our research. Without his support and encouragement this research would have been trivial. The author also thanks Y. Rohen Singh, HOD of Mathematics Department, NIT Manipur for his cooperation and guidance. We would also like to mention that it would not have been possible without the timely help and support of Electronics and Communication Engineering Department Labs, especially the Computer Lab.

REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, “Secure Spread Spectrum Watermarking for Multimedia”, IEEE Transaction on Image Processing, 6(12), 1673-1687, December, 1997.

[2] M.D.Swanson, M.Kobayashi and A.H.Tewfik, “Multimedia data embedding and watermarking technologies”, Proc. IEEE, Vol.86, pp. 1064-1087, June 1998.

[3] S.H.Low, N.F.Maxemchuk and A.M.Lapone, “Document identification for copyright protection using centroid detection”, IEEE Trans. Commun., vol.46, pp. 372-383, Mar. 1998.

[4] C.I.Podilchuk and E.J.Delp, “Digital Watermarking: Algorithms and Applications”, IEEE Signal Processing Magazine, pp.33-46, July 2001.

[5] Tao Peining and Eskicioglu Ahmet M, “An Adaptive Method for Image Recovery in the DFT Domain”, Journal of Multimedia, Vol. 1, No. 6 September 2006.

[6] Barni, F.Bartolini, A.Piva, “A DCT domain system for robust image watermarking”, IEEE Transactions on Signal Processing, 66, 357-372, 1998.

[7] Chu, W.C, “DCT based image watermarking using sub sampling”, IEEE Trans Multimedia 5, 34-38, 2003.

[8] M.Barni, M., Bartolini, F., V., Piva, “Improved wavelet based watermarking through pixel-wise masking”, IEEE Trans Image Processing 10, 783-791, 2001.

[9] Y.Wang, J.F.Doherty and R.E.Van Dyck, “A wavelet based watermarking algorithm for ownership verification of digital images”, IEEE Transactions on Image Processing, 11, No.2, pp. 77-88, February 2002.

[10] V.I. Gorodetski, L.J.Popyak, V.Samoilov and V.A.Skormin, “SVD-based Approach to Transparent Embedding Data into Digital Images”, International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001), St. Petersburg, Russia, May 21-23, 2001

[11] R.Liu, T.Tan, “An SVD-based watermarking scheme for protecting rightful ownership”, IEEE Trans. Multimedia, (4), 1, pp. 121-128, 2002.

[12] Sun, R., Sun, H., Yao, T, "A SVD and quantization based semi-fragile watermarking technique for image authentication", Proc. IEEE International Conf. Signal Processing, 2. 1592-1595, 2002.

[13] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, "SVD based digital image watermarking scheme", Pattern Recognition Letters 26, 1577-1586, 2005.

[14] D.V.S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition", Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems, Tulsa, OK, August 2002, pp. 264-267.

[15] R. Mehul and R.Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proceeding of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[16] Wu, C. and W. Hsieh, 2000, "Digital watermarking using zero tree of DCT", IEEE Trans. Consumer Electronics, vol. 46, No. 1, pp. 87-94.

[17] V.M. Potdar, S.Han and E.Chang, "A survey of digital image watermarking techniques", 3rd IEEE International conference on Industrial Informatics, pp. 709-716, 2005.

[18] J.R Hernandez, M. Amado and F.Perez Gonzalez, "DCT-Domain Watermarking Techniques for still Images: Detector Performance Analysis and a New Structure", in IEEE Trans. Image Processing, vol. 9, pp. 55-68, Jan, 2000.

[19] Y. Yang, X.Sun, H.Yang and C.T. Li, "A Removable Visible Image Watermarking Algorithm in DCT Domain", Journal of Electronic Imaging, vol. 17, No. 3, July-September, 2008.

[20] I.J.Cox, J.Lilian, F.T.Leighton and T.Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, pp. 1673-1687, January 1997.

[21] G.C. Langelaar and R.L. Langendijk, "Optional differential energy watermarking of DCT encoded images and video", IEEE Transactions on Image Processing, vol. 10, pp. 148-158, Jan. 2001.

[22] S. Murty and P. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique", International Journal of Computer Science and Network Security, Vol. 10, No. 10, October 2010.

[23] Shang-Lin Hsieh and Bin-Yuan Huang, "A Copyright Protection Scheme for Gray-Level Images Based on Image Secret Sharing and Wavelet Transformation", Proceedings of International Computer Symposium, Dec. 2004.

[24] Shang-Lin Hsieh and Lung-Yao Hsu, "A Copyright Protection Scheme for Color Image Using Secret Sharing and Wavelet Transform", Master Thesis, Tatung University, July 2005.

[25] Ju Liu, Xingang Zhang and Jiande Sun, "A new image watermarking scheme based on DWT and ICA", Proceedings of IEEE International Conference Neural Networks and Signal Processing, China, December 2003.

[26] Wang Hongjun and Li Na, "An algorithm of digital image watermark based on multiresolution wavelet analysis", IEEE International workshop on VLSI Design and Video Technology, China, May 2005.

[27] D. Taskovski, S. Bogdanova, and M. Bogdanov, "Digital watermarking in wavelet domain", First IEEE Balkan Conference on Signal Processing, Communication, Circuits, and Systems, 2000.

[28] G. Hai-ying, L.Guo-qiang, L.Xu, and X.Yin, "A robust watermark algorithm for jpeg2000 images", Fifth International Conference on Information Assurance and Security, 2009.

[29] D.R. Sans, "Identificao de propriedade em imagens com marcas d'gua no domino da transformada wavelet", Master's thesis, Universidade Federal do Paran-UFPR, 2008, in Portuguese.

[30] E.Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding data in all frequencies", Proceeding of the 2004 workshop on Multimedia and security, pp. 166-174, 2004.

[31] Md. Mahfuzur Rahman and Koichi Harada, "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", IJCHNS International Journal of Computer Science and Network Security, Vol. 6, No. 2A, February 2006.

[32] M. Hamad Hassan, and A.A.M.Gilani, "A Fragile Watermarking Scheme for Color Image Authentication", International Journal of Applied Science, Engineering and Technology, Vol. 1, No. 3, pp.-156-160, 2005.

[33] M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain", University of Bonn Germany, Tech. Rep., 2006.

[34] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection, Artech House, 2003.

[35] Xiangui Kang, Jiwu Huang, and Wenjun Zeng, "Improving Robustness of Quantization-Based Image Watermarking via Adaptive Receiver", IEEE Transactions on Multimedia, Vol. 10, No. 6, pp. 953-959, October 2008.

[36] X.Kang, J.Hang, and Y.Q.Shi, Y.Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and jpeg compression", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, pp. 776-786, August 2003.

[37] J. Huang, Y.Q.Shi, "Reliable information bit hiding", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 10, pp. 916-920, 2002.

[38] C.Lu, H.Yuan, and M. Liao, "Multipurpose watermarking for image authentication and protection", IEEE Transactions on Image Processing, Vol. 10, No. 10, pp. 1579-1592, October 2001.

[39] Ruizhen Liu, Tieniu Tan, "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Transaction on Multimedia, Vol. 4, No. 1, pp. 121-128, March 2002.

[40] Wei Lu, Hongtao Lu, "Robust watermarking based on sub-sampling and nonnegative matrix factorization", Informatica, Vol. 19, No. 4, pp. 555-566, December 2008.

[41] C. Lin, M.Wu, Y.M. Lui, J.A Bloom, M.L. Miller, I .J. Cox, "Rotation, Scale, and Translation Resilient Public Watermarking for Images", IEEE Transactions on Image Processing, Vol. 10, No. 5, pp. 767-782, 2001.

[42] R. N. Bracewell, "The Fourier Transform and Its Applications", New York: McGraw-Hill, 1986.

[43] N. Pantuwong and N. Chotikakamthorn, "Line watermark embedding method for affine transformed images", ISSPA 2007, PP. 1-4, 2007.

[44] S. Riaz, M. Y. Javel, and M. A. Anjum, "Invisible watermarking scheme in spatial and frequency domains", International Conference on Emerging Technologies, 2008.

[45] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No. 9, pp. 740-746, 2007.

[46] R. A. Ghazy, N.A. El-Fishawy, M.M. Hadhoud, M.I. Dessouky, and F.E.A.E.-S. Samie, "An efficient block-by-block SVD-based image watermarking scheme", National Radio Science Conference, pp. 1-9, 2007.

[47] C.Hsieh, & P. Tsou, "Blind Cepstrum Domain Audio Watermarking Based on Time Energy Features", 4th International Conference on Digital Signal Processing, 705-708, 2004.

[48] B. Vladimir, K.E.Rao, "An Efficient Implementation of the Forward and Inverse MDCT in MPEG Audio Coding", IEEE Signal Processing Letters, Vol. 8, No. 2, 2005.

[49] Chung K, Yang W, Huang Y, Wu S, Hsu Yu-Chiao, "On SVD-based watermarking algorithm", Applied Mathematics and Computation Elsevier, 188, 54-57, 2007.

[50] Jieh-Ming Shieh, Der-Chyuan Lou and Ming-Chang Chang, "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards and Interfaces 28, 428-440, 2006.

[51] I.J.Cox, M.L. Miller, J.A.Bloom,J.Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008.

[52] J.Liu and X.He, "A review study on digital watermarking", 1st International Conference on Information and Communication Technologies, pp. 337-341, 2005.

[53] Edin Muharemagic and Borko Furht "A survey of watermarking techniques and applications" 2001.

[54] J. Fridrich, "Image watermaking for tamper detection", in Proc. IEEE International Conference Image Processing, Chicago, IL, Oct. 1998, pp. 404-408.

[55] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking health care".

[56] Edin Muharemagic and Borko Furht "Survey of watermarking Techniques and Applications".

[57] Friedman, G.L., "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp. 905-910.

[58] F. Hartung, J.K. Su., and B.Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks", pp. 147-158, 1999.

[59] Katzenbeisser S. and Petitcolas F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Aetech House, UK, 2000.